Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®

Discrete Mathematics 278 (2004) 139–149

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

# Generator polynomials of characteristic ideal of maximal periodic arrays over Galois rings☆

Lei Hu[a,*], Dingyi Pei[b]

[a] *State Key Laboratory of Information Security, Graduate School, Chinese Academy of Sciences, 19A Yuqian Road, Beijing 100039, People's Republic of China*

[b] *Department of Mathematics, Guangzhou University, Guangzhou 510405, People's Republic of China*

Received 5 April 2001; received in revised form 20 June 2003; accepted 27 June 2003

**Abstract**

In [Maximal periodic two-dimensional arrays over Galois rings, preprint, 2000, submitted for publication] we obtain a trace expression for maximal periodic two-dimensional arrays over Galois rings. In this paper, based on the trace expression, we deduce a complete characterization for the generator polynomials of the characteristic ideal of maximal periodic arrays. This characterization explicitly gives a simple polynomial construction method for such characteristic ideals.


*MSC:* 94A55; 13M10; 11T71

*Keywords:* Maximal periodic array; Galois ring; Characteristic ideal; Generator polynomial

## 1. Introduction

In [4] we deduce the upper bound of the periods of two-dimensional periodic arrays over Galois rings and obtain a trace expression for maximal periodic arrays over Galois rings (Theorem 1 quoted below). Such arrays are analogies of maximal periodic arrays over finite fields (m-arrays [7,11]), and may be used in communication such as two-dimensional position location, mask configurations [11] and digital signal sequences [1,12,13], in coding theory [2,5,10], and in cryptographic key generation [3].

☆ This work is supported by the National Natural Science Foundation of China (Grant No. 90104034), the Guangdong Provincial Natural Science Foundation of China (Grant No. 990336) and the National High Technology Research and Development Program of China (Grant No. 2002AA141020).

* Corresponding author.
*E-mail addresses:* hu@is.ac.cn, gnuleihu@sina.com (L. Hu).

0012-365X/$ - see front matter 
doi:10.1016/j.disc.2003.06.001

However, the expression in Theorem 1 involves elements of an extension ring, which are common roots of the characteristic ideal of maximal periodic arrays, and this may be inconvenient for applications. In this paper we consider the generator polynomials of the characteristic ideal of such maximal periodic arrays and give a complete characterization of the generator polynomials. This characterization explicitly gives a simple polynomial construction method for such characteristic ideals.

## 2. Preliminaries

Let $R = GR(p^e, d)$ be the Galois ring with characteristic $p^e$ and residue field $F = F_q$, where $q = p^d$. $R$ is a local ring with maximal ideal $pR$. There exists a unique unramified extension ring $S$ of $R$ of degree $t$, and $S = GR(p^e, dt)$. Let $\bar{\ }$ denote the natural homomorphism mod $p$ from $S$ to $E = F_{q^t} (\cong S/pS)$ and the one from $R$ to $F_q (\cong R/pR)$. The two homomorphisms can be naturally extended to a homomorphism from $S[x]$ to $E[x]$ and a one from $R[x]$ to $F[x]$, respectively. For $a, b \in R$, let $a \equiv b \pmod p$ denote $a - b \in pR$. For the details of Galois ring, see, e.g., [9].

Let $\Sigma_S = \{a \in R : a^{q^t} = a\}$ be the Teichmuller system of $S$. Then $\Sigma_S \setminus \{0\}$ is a cyclic multiplicative group of order $q^t - 1$, and $\overline{\Sigma_S} = F_{q^t}$. Any $a \in S$ has a unique $p$-adic expression $a = a_0 + pa_1 + \cdots + p^{e-1}a_{e-1}$, where $a_i \in \Sigma_S$. The Frobenius automorphism $\sigma$ of $S$ over $R$ acts on $a$ by $\sigma(a) = a_0^q + pa_1^q + \cdots + p^{e-1}a_{e-1}^q, a_i \in \Sigma_S$. The Galois group $\mathrm{Gal}(S/R)$ of $S$ over $R$, which is the set of all automorphisms of $S$ fixing elements of $R$, is a cyclic group of order $t$ and is generated by $\sigma$. The trace map $\mathrm{Tr}_R^S$ of $S$ over $R$ acts on $a$ by $\mathrm{Tr}_R^S(a) = a + \sigma(a) + \cdots + \sigma^{t-1}(a)$. $\sigma$ induces the Frobenius automorphism of $F_{q^t}$ over $F_q$, which is denoted by $\bar{\sigma}$, as follows:

$$\bar{\sigma}(\bar{a}) = \overline{\sigma(a)} = \overline{a_0^q} = \overline{a_0}^q = \bar{a}^q.$$

We consider two-dimensional arrays $A = (a_{kl})_{(k,l)\in Z^2}$ over $R$, $a_{kl} \in R$. Let $R[x, y]$ be the polynomial ring over $R$ of two indeterminates. Let $\Omega_R$ be the set of all arrays over $R$. $\Omega_R$ is naturally an $R[x, y]$-module where $f(x, y) = \sum c_{ij}x^i y^j \in R[x, y]$ acts on $A = (a_{kl})_{(k,l)\in Z^2} \in \Omega_R$ to get $fA = (\sum c_{ij}a_{i+k,j+l})_{(k,l)\in Z^2} \in \Omega_R$. For an ideal $I$ of $R[x, y]$ and a subset $G$ of $\Omega_R$, let $\Omega(I, R)$ denote the set of arrays over $R$ annihilated by all polynomials in $I$, and $I(G, R)$ the set of polynomials of $R[x, y]$ annihilating all arrays in $G$. $\Omega(I, R)$ is an $R[x, y]$-module, and $I(G, R)$ is an ideal of $R[x, y]$. $I(G, R)$ is called the characteristic ideal of the array set $G$. If $G = \{A\}$ is a set of a single array $A$, then $I(G, R)$, also written as $I(A, R)$, is called the characteristic ideal of $A$. An ideal $I$ of $R[x, y]$ is called periodic if $I$ contains polynomials of the form $x^r - 1$ and $y^s - 1$ with $r, s > 0$. An array $A$ is called periodic if its characteristic ideal $I(A, R)$ is periodic.

For a periodic array $A = (a_{kl})_{(k,l)\in Z^2}$, a vector $(r, s) \in Z^2$ such that $a_{r+k,s+l} = a_{kl}$ holds for any $(k, l) \in Z^2$ is called a period vector of $A$. All period vectors of $A$ form a lattice of $Z^2$ of rank 2, denoted by $L_A$. The absolute value of the determinant of the $2 \times 2$ matrix formed by the 2 vectors of any $Z$-basis of this lattice is called the period of $A$, denoted by $\mathrm{per}(A)$, which is independent on the choice of $Z$-basis since two such bases are $Z$-linear equivalent. $L_A$ always has a so-called x-standard $Z$-basis of the form $\{(u, 0), (w, v)\}$, where $u, v > 0$ and $0 \leqslant w < u$. Obviously, $\mathrm{per}(A) = |Z^2/L_A| = uv$.

**Theorem 1** (Hu and Pei [4]). *Let $I$ be a periodic ideal of $R[x,y]$, $\dim_F \Omega(\bar{I},F)=t$, $R=GR(p^e,d)$, $S=GR(p^e,dt)$, $F=F_q=F_{p^d}$, and $E=F_{q^t}$. Then for any $A\in\Omega(I,R)$,*

$$\mathrm{per}(A)\leqslant p^{2(e-1)}(q^t-1) \tag{1}$$

*and that the equality in (1) holds for some $A\in\Omega(I,R)$ if and only if there exist $\alpha,\beta\in S\setminus pS$ such that*

(i) $\{\bar{\alpha}^i\bar{\beta}^j|(i,j)\in Z^2\}=E\setminus\{0\}$;
(ii) *Set $\alpha=\alpha_0(1+p\alpha_1+\cdots+p^{e-1}\alpha_{e-1})$, $\beta=\beta_0(1+p\beta_1+\cdots+p^{e-1}\beta_{e-1})$, $\alpha_i,\beta_i\in\Sigma_S$. Then as elements of $E$, $\{\overline{\alpha_1},\overline{\beta_1}\}$ is $F_p$-linear independent, and in addition, if $p=2<e$, no $F_2$-linear combination of $\overline{\alpha_1}$ and $\overline{\beta_1}$ is 1; and*
(iii) *For any $A=(a_{kl})_{(k,l)\in Z^2}\in\Omega(I,R)$, there exist $\theta\in S$ such that for any $(k,l)\in Z^2$,*

$$a_{kl}=\mathrm{Tr}_R^S(\theta\alpha^k\beta^l). \tag{2}$$

*Furthermore, if the equality in (1) holds, then for general $0\neq A\in\Omega(I,R)$, $\mathrm{per}(A)=p^{2(k-1)}(q^t-1)$, where $k$ is the minimal integer $k$ such that $1\leqslant k\leqslant e$ and $\theta\in p^{e-k}S$. ($k$ is also the minimal integer $k$ such that $1\leqslant k\leqslant e$ and that $\{a_{kl}|(k,l)\in Z^2\}\subseteq p^{e-k}R$.)*

**Definition 1.** Let $I$ be a periodic ideal. If the equality in (1) holds for some $A\in\Omega(I,R)$, then $I$ is called maximal periodic and any $A\in\Omega(I,R)$ with $\mathrm{per}(A)=p^{2(e-1)}(q^t-1)$ is called a maximal periodic array.

## 3. Generator polynomials of characteristic ideal of maximal periodic arrays

**Lemma 1.** *Let $F=F_q$, $E=F_{q^t}$, $\alpha,\beta\in E\setminus\{0\}$, and $F_{q^u}$ and $F_{q^v}$ be the minimal subfield of $E$ containing $\alpha$ and $\beta$, respectively. Suppose $E\setminus\{0\}$ is generated by $\alpha$ and $\beta$ as a multiplicative group. Then $u=t$ or $v=t$.*

**Proof.** The homomorphism of groups from the outer direct product $\langle\alpha\rangle\times\langle\beta\rangle$ to $E\setminus\{0\}$, mapping $(\alpha^i,\beta^j)$ to $\alpha^i\beta^j$, shows that $|E\setminus\{0\}|=|\langle\alpha\rangle|\cdot|\langle\beta\rangle|\cdot|\langle\alpha\rangle\cap\langle\beta\rangle|^{-1}$. Let $rd$ and $sd$ be the order of $\alpha$ and $\beta$, respectively, and $\gcd(r,s)=1$. Set $h=q^t-1$. Since $E\setminus\{0\}$ is a cyclic group generated by primitive element, say $\theta$, we have $\langle\alpha\rangle=\langle\theta^{h/rd}\rangle$, $\langle\beta\rangle=\langle\theta^{h/sd}\rangle$ and $\langle\alpha\rangle\cap\langle\beta\rangle=\langle\theta^{h/d}\rangle$. Thus, $h=rd\cdot sd\cdot d^{-1}=\mathrm{lcm}(\mathrm{ord}(\alpha),\mathrm{ord}(\beta))$. Set $u=ac$, $v=bc$, and $\gcd(a,b)=1$. Then $q^t-1$ divides $\mathrm{lcm}(q^{ac}-1,q^{bc}-1)$. Since $u$ and $v$ divides $t$, $abc$ divides $t$. From $q^{abc}-1\leqslant(q^{ac}-1)(q^{bc}-1)$, we have $a=1$ or $b=1$. If $a=1$, then $F_{q^t}=F[\alpha][\beta]=F_{q^c}[\beta]=F_{q^{bc}}$, and we have $bc=t$. If $b=1$, similarly, we have $ac=t$. □

**Definition 2.** An $(n,m;R)$-pair is a pair of polynomials $f(x)\in R[x]$ and $g(x,y)\in R[x,y]$ such that $f(x)$ is monic and of degree $n$, $g(x,y)$ is of the form

$$y^m+\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}g_{ij}x^iy^j,$$

$\bar{f}(x)$ is irreducible over $F = R/pR$, $\bar{f}(0) \neq 0$, and that $\bar{g}(x, y)$ is irreducible over $F[x]/(\bar{f}(x))$ as a polynomial of $y$, $\bar{g}(x, 0) \neq 0$ as an element in $F[x]/(\bar{f}(x))$.

**Theorem 2.** *With the notation $R, t, I, \alpha, \beta, \alpha_i, \beta_i, F, E$ be as in Theorem* 1 *such that the equality in* (1) *and* (2) *hold. Then there exist a factor $n$ of $t$ and an $(n, t/n; R)$-pair $(f(x), g(x, y))$ such that*

$$I = \langle f(x), g(x, y)\rangle \quad \text{and} \quad f(\alpha) = g(\alpha, \beta) = 0,$$

*or*

$$I = \langle f(y), g(y, x)\rangle \quad \text{and} \quad f(\beta) = g(\beta, \alpha) = 0.$$

**Proof.** Let $F_{q^u}$ and $F_{q^v}$ be the minimal subfields of $E$ containing $\overline{\alpha_0}$ and $\overline{\beta_0}$, respectively. By Lemma 1, $u = t$ or $v = t$. Let $\Sigma^{(i)}$ be the Teichmuller system of $GR(p^e, di)$, and $u'$ and $v'$ be the minimal superscripts $i$ and $j$ such that $\{\alpha_1, \ldots, \alpha_{e-1}\} \subseteq \Sigma^{(i)}$ and $\{\beta_1, \ldots, \beta_{e-1}\} \subseteq \Sigma^{(j)}$, respectively. Then $\{\overline{\alpha_1}, \ldots, \overline{\alpha_{e-1}}\} \subseteq F_{q^{u'}}$, $\{\overline{\beta_1}, \ldots, \overline{\beta_{e-1}}\} \subseteq F_{q^{v'}}$, and $u'$ and $v'$ divide $t$. Thus, $u'$ divides $u$, or $v'$ divides $v$. Without loss of generality, we suppose $u'$ divides $u$ and $u = n$. By Hensel's Lemma, we can lift the minimal polynomial of $\overline{\alpha_0}$ over $F$, which is of degree $n$, to get a monic polynomial over $R$ and of degree $n$, say $f(x)$, such that $f(\alpha) = 0$. Since $\bar{f}(\overline{\alpha_0}) = \overline{f(\alpha)} = 0$, $\bar{f}(x)$ is the irreducible minimal polynomial of $\overline{\alpha_0}$ over $F$. Set $S_1 = GR(p^e, dn)$. Then $R[\alpha] = S_1$, and any element $b$ of $S_1$ is uniquely represented as $b = \sum_{i=0}^{n-1} b_i \alpha^i$, $b_i \in R$. If $n = t$, set $m = 1$ and $G(y) = y^m + \sum_{j=0}^{m-1} b_j y^j = y - \beta$ be the minimal polynomial of $\beta$ over $S_1$. If $n < t$, by Lemma 1, $v'$ divides $t = v$. By Theorem 1(i), $F_{q^n}[\overline{\beta_0}] = F[\overline{\alpha_0}][\overline{\beta_0}] = F[\overline{\alpha_0}, \overline{\beta_0}] = F_{q^t}$, set $m = t/n$. By Hensel's Lemma, we can lift the minimal polynomial of $\overline{\beta_0}$ over $F_{q^n}$ to get a monic polynomial over $S_1$ and of degree $m$, say $G(y)$, such that $G(\beta) = 0$. Similarly, $\bar{G}(y)$ is irreducible over $F_{q^n}$. Set

$$G(y) = y^m + \sum_{j=0}^{m-1} b_j y^j, \quad b_j = \sum_{i=0}^{n-1} g_{ij}\alpha^i, \ \ g_{ij} \in R$$

and

$$g(x, y) = y^m + \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} g_{ij} x^i y^j.$$

Then $g(\alpha, \beta) = 0$. For any $A \in \Omega(I, R)$, by Theorem 1(iii), $A = \mathrm{Tr}_R^S(A_1)$, $A_1 = (\theta \alpha^k \beta^l)_{(k,l)\in Z^2}$. From $f(\alpha) = g(\alpha, \beta) = 0$, we have that $A_1$ is annihilated by $f(x)$ and $g(x, y)$. So, $A = \sum_{\sigma \in \mathrm{Gal}(S/R)} \sigma(A_1)$ is also annihilated by $f(x)$ and $g(x, y)$, and $A \in \Omega(J, R)$, where $J = \langle f(x), g(x, y)\rangle$. This implies $\Omega(I, R) \subseteq \Omega(J, R)$. By Theorem 1(iii), there exist at most $|S| = q^{et}$ arrays in $\Omega(I, R)$. However, each array $B$ in $\Omega(J, R)$ is uniquely determined by the entries of $B$ over

$$\Gamma(J) = \{(i, j) \in Z^2 \mid 0 \leqslant i < n, 0 \leqslant j < m\}$$

and $|\Omega(J, R)| = |R|^{nm} = q^{enm} = q^{et}$. So, $\Omega(I, R) = \Omega(J, R)$ and by Lu [8], $I = J$. The theorem is proved. □

In the sequel, let $(f,g)$ be an $(n,m;R)$-pair, $\alpha,\beta\in S=GR(p^e,dnm)$, and $I=\langle f(x),g(x,y)\rangle$. Assume $f(\alpha)=g(\alpha,\beta)=0$, and express $\alpha$ and $\beta$ as in Theorem 1(ii). We will deduce a sufficient and necessary condition that $f(x)$ and $g(x,y)$ generate a maximal periodic ideal.

By the $p$-adic expression for elements in $R$, we have the following $p$-adic expressions for $f(x)$ and $g(x,y)$:

$$f(x)=f_0(x)+pf_1(x)+\cdots+p^{e-1}f_{e-1}(x), \tag{3}$$

$$g(x,y)=g_0(x,y)+pg_1(x,y)+\cdots+p^{e-1}g_{e-1}(x,y), \tag{4}$$

where $f_i(x)$ and $g_i(x,y)$ have coefficients in $\Sigma_R$,

$$\deg f_i(x)<\deg f_0(x)=n,\ \deg_y g_i(x,y)<\deg_y g_0(x,y)=m,\quad \forall i\geqslant 1$$

and

$$\deg_x g_i(x,y)<n,\quad \forall i\geqslant 0.$$

For convenience, we say $f_i(x)$ and $g_i(x,y)$ are the $i$th $p$-adic component of $f(x)$ and $g(x,y)$, respectively.

Let $h(x,y)=\sum_{(i,j)\in D}b_{ij}x^iy^j$ be an arbitrary polynomial in $R[x,y]$, where $D$ is a finite index set. Define $\Phi h\in R[x,y]$ as

$$\Phi h(x,y)=\sum q!\left(p\prod_{(i,j)\in D}k_{ij}!\right)^{-1}\prod_{(i,j)\in D}(b_{ij}^{k_{ij}}x^{ik_{ij}}y^{jk_{ij}}), \tag{5}$$

where the sum is over the tuples of nonnegative integers $k_{ij}$ satisfying $\sum_{(i,j)\in D}k_{ij}=q$, $k_{ij}<q$ and $p^{d-1}|k_{ij}$ (recall that $q=p^d$) and define $\Psi h\in R[x,y]$ as

$$\Psi h(x,y)=\sum(p-1)!\left(\prod_{(i,j)\in D}k_{ij}!\right)^{-1}\prod_{(i,j)\in D}(b_{ij}^{k_{ij}}x^{ik_{ij}}y^{jk_{ij}}), \tag{6}$$

where the sum is over the tuples of nonnegative integers $k_{ij}$ satisfying $\sum_{(i,j)\in D}k_{ij}=p$ and $k_{ij}<p$.

**Lemma 2.** (i) [14]

$$h(x,y)^q\equiv h(x^q,y^q)+p\Phi h(x,y)\,(\mathrm{mod}\ p^2). \tag{7}$$

(ii) *Let* $0\leqslant j<p$, $k\geqslant 1$, *and* $(jp^d)!=p^uv$, $\gcd(v,p)=1$. *Then*

$$u=j(p^d-1)/(p-1),\quad v\equiv(-1)^{jd}j!\,(\mathrm{mod}\ p).$$

(iii) *Let* $0\leqslant j_0,j_1,\ldots,j_t<p$ *and* $j_0+j_1+\cdots+j_t=p$. *Then*

$$\frac{(p^d)!}{p(j_0p^{d-1})!\cdots(j_tp^{d-1})!}\equiv\frac{(p-1)!}{j_0!j_1!\cdots j_t!}\,(\mathrm{mod}\ p).$$

(iv)

$$\Phi\bar{h}(x,y)=\bar{\Psi h}(x,y)^{p^{d-1}}. \tag{8}$$

**Proof.** It is trivial that (iii) follows (ii), and that (iv) follows (iii) and (i). To prove (i), we expand

$$h(x,y)^q = \left(\sum_{(i,j)\in D} b_{ij}x^i y^j\right)^q = \sum q! \left(\prod_{(i,j)\in D} k_{ij}!\right)^{-1} \prod_{(i,j)\in D} (b_{ij}^{k_{ij}} x^{ik_{ij}} y^{jk_{ij}}),$$

where the sum is over the tuples of nonnegative integers $k_{ij}$ satisfying $\sum_{(i,j)\in D} k_{ij} = q$. By Lidl and Niederreiter [6, Lemma 6.39], the index of the maximal power of $p$ dividing $q!(\prod_{(i,j)\in D} k_{ij}!)^{-1}$ is 0 if and only if some $k_{ij}$ is $q$; and is $\geqslant 2$ if some $k_{ij}$ is not divided by $p^{d-1}$. This proves (i).

To prove (ii), let $\Pi = \{1,2,\ldots,jp^d\}$. Since for any $0 \leqslant i < jp^{d-1}$, the product of the integers $1+pi, 2+pi, \ldots$, and $p-1+pi$ is congruent to $-1$ modulo $p$, the product of all integers in $\Pi$ which are prime with $p$ is congruent to $(-1)^{jp^{d-1}} \equiv (-1)^j$ modulo $p$. The product of the integers in $\Pi$ which are divided by $p$ is $p^{jp^{d-1}}(jp^{d-1})!$. By induction on $d$, we have

$$u = jp^{d-1} + jp^{d-2} + \cdots + jp + j = j(p^d - 1)/(p-1)$$

and

$$v \equiv (-1)^{jd} j! \,(\mathrm{mod}\ p). \qquad \square$$

Let $\pi$ denote the automorphism of $F_q[x,y]$ mapping $\sum a_{ij}x^i y^j$ to $\sum a_{ij}^p x^i y^j$. Let $f_0^{(x)}(x)$ be the formal differential of $f_0(x)$, and $g_0^{(x)}(x,y)$ and $g_0^{(y)}(x,y)$ be the formal partial differentials of $g_0(x,y)$.

**Lemma 3.**

$$\alpha_1^p \equiv \frac{\Psi f_0(\alpha_0) - \pi f_1(\alpha_0^p)}{\alpha_0^p \pi f_0^{(x)}(\alpha_0^p)} \,(\mathrm{mod}\ p) \tag{9}$$

*and*

$$\beta_1^p \equiv \frac{\Psi g_0(\alpha_0,\beta_0) - \pi g_1(\alpha_0^p,\beta_0^p) - \alpha_0^p \alpha_1^p \pi g_0^{(x)}(\alpha_0^p,\beta_0^p)}{\beta_0^p \pi g_0^{(y)}(\alpha_0^p,\beta_0^p)} \,(\mathrm{mod}\ p). \tag{10}$$

**Proof.** By the fact that a root of an irreducible polynomial over a finite field is not a root of its formal differential, we have $f_0^{(x)}(\alpha_0) \neq 0 \,(\mathrm{mod}\ p)$ and $g_0^{(y)}(\alpha_0,\beta_0) \neq 0 \,(\mathrm{mod}\ p)$. Let $\sigma$ be the Frobenius map of $GR(p^e, dn)$ over $R$. For any $i = 0,1,\ldots,n-1$,

$$\sigma^i(\alpha) = \alpha_0^{q^i} + p\alpha_0^{q^i}\alpha_1^{q^i} + \cdots + p^{e-1}\alpha_0^{q^i}\alpha_{e-1}^{q^i}$$

is a root of $f(x)$. By (3), we have

$$f_0(\alpha_0^{q^i} + p\alpha_0^{q^i}\alpha_1^{q^i} + \cdots) + pf_1(\alpha_0^{q^i} + p\alpha_0^{q^i}\alpha_1^{q^i} + \cdots) \equiv 0 \,(\mathrm{mod}\ p^2),$$

Expanding this equation,

$$f_0(\alpha_0^{q^i}) + p\alpha_0^{q^i}\alpha_1^{q^i} f_0^{(x)}(\alpha_0^{q^i}) + pf_1(\alpha_0^{q^i}) \equiv 0 \,(\mathrm{mod}\ p^2). \tag{11}$$

Since $f_0(\alpha_0^{q^i}) \equiv 0 \pmod p$ and $q \geqslant 2$, $f_0(\alpha_0^{q^i})^q \equiv 0 \pmod{p^2}$. In particular, $f_0(\alpha_0)^q \equiv 0 \pmod{p^2}$. By (7),

$$f_0(\alpha_0^q) + p\Phi f_0(\alpha_0) \equiv 0 \pmod{p^2}. \tag{12}$$

By (11) and (12),

$$f_1(\alpha_0^q) + \alpha_0^q \alpha_1^q f_0^{(x)}(\alpha_0^q) - \Phi f_0(\alpha_0) \equiv 0 \pmod p.$$

By Lemma 2(iv), taking the $p$th power on the both sides, we have

$$\pi f_1(\alpha_0^{qp}) + \alpha_0^{qp} \alpha_1^{qp} \pi f_0^{(x)}(\alpha_0^{qp}) - \Psi f_0(\alpha_0)^q \equiv 0 \pmod p$$

and then taking the $q$th root on the both sides gives us

$$\pi f_1(\alpha_0^p) + \alpha_0^p \alpha_1^p \pi f_0^{(x)}(\alpha_0^p) - \Psi f_0(\alpha_0) \equiv 0 \pmod p.$$

This deduces (9). The proof to (10) is similar. □

For an $(n, m; F_q)$-pair $(f_0(x), g_0(x, y))$, we define $\Lambda f_0 \in F_q[x]$ such that

$$\Lambda f_0 \equiv (\Phi f_0)^{q^{nm-1}} \pmod{\langle f_0 \rangle} \tag{13}$$

and define $\Lambda g_0 \in F_q[x, y]$ such that

$$\Lambda g_0 \equiv (\Phi g_0)^{q^{nm-1}} \pmod{\langle f_0, g_0 \rangle}, \tag{14}$$

where $\Phi f_0, \Phi g_0 \in F_q[x, y]$ are defined similarly as in (5).

**Definition 3.** Assume $(f_0(x), g_0(x, y))$ is an $(n, m; F_q)$-pair and $f_1(x), g_1(x, y) \in F_q[x, y]$. We say that $(f_1, g_1)$ is independent on $(f_0, g_0)$ if for any $(0, 0) \neq (a, b) \in F_p^2$,

$$\begin{aligned}&(axg_0^{(x)} + byg_0^{(y)})f_1 - (axf_0^{(x)})g_1 \\ &\quad \neq (axg_0^{(x)} + byg_0^{(y)})\Lambda f_0 - (axf_0^{(x)})\Lambda g_0 \pmod{\langle f_0, g_0 \rangle}\end{aligned} \tag{15}$$

and in addition in the case of $p = 2 < e$ if

$$f_1 \neq \Lambda f_0 + xf_0^{(x)} \pmod{\langle f_0 \rangle}, \tag{16}$$

$$\begin{aligned}&g_0^{(x)} f_1 + f_0^{(x)} g_1 \\ &\neq g_0^{(x)} \Lambda f_0 + f_0^{(x)} \Lambda g_0 + y f_0^{(x)} g_0^{(y)} \pmod{\langle f_0, g_0 \rangle}\end{aligned} \tag{17}$$

and

$$\begin{aligned}&(xg_0^{(x)} + yg_0^{(y)})f_1 + xf_0^{(x)} g_1 \\ &\quad \neq (xg_0^{(x)} + yg_0^{(y)})\Lambda f_0 + xf_0^{(x)} \Lambda g_0 + xy f_0^{(x)} g_0^{(y)} \pmod{\langle f_0, g_0 \rangle}.\end{aligned} \tag{18}$$

**Theorem 3.** *Assume $(f(x), g(x, y))$ is an $(n, m; R)$-pair and $I = \langle f(x), g(x, y) \rangle$. Represent $f(x)$ as in (3) and $g(x, y)$ in (4). Then $I$ is a maximal periodic ideal if and*

*only if*

(i) *Let $u$ be the period of $\overline{f_0}(x)$ and $v=(q^{nm}-1)/u$, then for any prime divisor $r$ of $v$, $y^{v/r}$ is not congruent to any monic monomial of $x$ modulo $\langle\overline{f_0},\overline{g_0}\rangle$; and*
(ii) *As polynomials over $F_q$, $(\overline{f_1},\overline{g_1})$ is independent on $(\overline{f_0},\overline{g_0})$.*

**Proof.** By Lemma 2 of Hu and Pei [4], under the hypothesis of the theorem, there exist $\alpha,\beta\in GR(p^e,dnm)$ such that $f(\alpha)=g(\alpha,\beta)=0$ and Theorem 1(iii) holds. We prove the statements (i) and (ii) correspond to Theorem 1(i) and (ii), respectively.

Set $E=F_{q^{nm}}$. Let $v'$ be the minimal positive integer such that $\bar{\beta}^{v'}$ is equal to some power of $\bar{\alpha}$, i.e., such that $y^{v'}$ is congruent to some monic monomial of $x$ modulo $\langle\overline{f_0},\overline{g_0}\rangle$. Since $\bar{\alpha}$ is of order $u$, for any two different tuples $(i,j)$ and $(i',j')$ with $0\leqslant i,i'<u$ and $0\leqslant j,j'<v'$, we have $\bar{\alpha}^i\bar{\beta}^j\neq\bar{\alpha}^{i'}\bar{\beta}^{j'}$. Thus, the cardinality of $\{\bar{\alpha}^i\bar{\beta}^j:(i,j)\in Z^2\}$ is $uv'$, and Theorem 1(i) is equivalent to say that $v'=v$.

By Lemma 2(iv) and (13),

$$\begin{aligned}\Psi f_0(\alpha_0)\equiv\Psi f_0(\alpha_0)^{q^{nm}}&\equiv(\Psi f_0(\alpha_0)^{q/p})^{q^{nm-1}p}\equiv\Phi f_0(\alpha_0)^{q^{nm-1}p}\\&\equiv\Lambda f_0(\alpha_0)^p\,(\mathrm{mod}\ p)\end{aligned}$$

and similarly, $\Psi g_0(\alpha_0,\beta_0)\equiv\Lambda g_0(\alpha_0,\beta_0)^p\,(\mathrm{mod}\ p)$. By Lemma 3 and taking the $p$th root on the both sides of (9) and (10), we have

$$\alpha_1\equiv\frac{A}{C}\,(\mathrm{mod}\ p),\quad\text{and}\quad\beta_1\equiv\frac{B}{D_2}-\frac{D_1}{D_2}\frac{A}{C}\,(\mathrm{mod}\ p),$$

where

$$A=\Lambda f_0(\alpha_0)-f_1(\alpha_0),\quad B=\Lambda g_0(\alpha_0,\beta_0)-g_1(\alpha_0,\beta_0)$$

and

$$C=\alpha_0 f_0^{(x)}(\alpha_0),\quad D_1=\alpha_0 g_0^{(x)}(\alpha_0,\beta_0),\quad D_2=\beta_0 g_0^{(y)}(\alpha_0,\beta_0).$$

Then $\overline{\alpha_1}$ is $F_p$-linear independent with $\overline{\beta_1}$ if and only if for any $(0,0)\neq(a,b)\in F_p^2$,

$$b\frac{A}{C}-a\left(\frac{B}{D_2}-\frac{D_1}{D_2}\frac{A}{C}\right)\neq 0\,(\mathrm{mod}\ p),$$

reformulating it gives us

$$\begin{aligned}&(a\alpha_0 g_0^{(x)}(\alpha_0,\beta_0)+b\beta_0 g_0^{(y)}(\alpha_0,\beta_0))f_1(\alpha_0)-(a\alpha_0 f_0^{(x)}(\alpha_0))g_1(\alpha_0,\beta_0)\\&\quad\neq(a\alpha_0 g_0^{(x)}(\alpha_0,\beta_0)+b\beta_0 g_0^{(y)}(\alpha_0,\beta_0))\Lambda f_0(\alpha_0)\\&\qquad-(a\alpha_0 f_0^{(x)}(\alpha_0))\Lambda g_0(\alpha_0,\beta_0)\,(\mathrm{mod}\ p),\end{aligned}$$

this gives (15). In addition, when $p=2<e$, if no $F_2$-linear combination of $\overline{\alpha_1}$ and $\overline{\beta_1}$ is 1, then,

$$\frac{A}{C}\neq 1\,(\mathrm{mod}\,2),\quad\frac{B}{D_2}-\frac{D_1}{D_2}\frac{A}{C}\neq 1\,(\mathrm{mod}\,2),\quad\frac{A}{C}+\frac{B}{D_2}-\frac{D_1}{D_2}\frac{A}{C}\neq 1\,(\mathrm{mod}\,2),$$

processing similarly deduces respectively formulas (16)–(18). □

**Remark 1.** The ideal $\langle \overline{f_0}(x), \overline{g_0}(x,y)\rangle$ in Theorem 3(i) is a maximal periodic ideal of $F_q[x,y]$. Such an ideal is an analogy of a primitive polynomial over $F_q$ and is a zero-dimensional prime ideal of $F_q[x,y]$ with nonzero common zero of maximal period, where the period of $(\alpha,\beta)$ is defined as the cardinality of $\{\alpha^i\beta^j \mid (i,j)\in Z^2\}$.

**Lemma 4.** *Let $(f_0(x), g_0(x,y))$ be an $(n,m;F_q)$-pair. Assume $f_1(x), g_1(x,y)\in F_q[x,y]$, $\deg f_1 < n$, $\deg_x g_1 < n$, and $\deg_y g_1 < m$. Then there are exactly $q^n-2$ choices of $f_1$ and $q^{nm}-4$ choices of $g_1$ such that $(f_1,g_1)$ is independent on $(f_0,g_0)$ if $2=p<e$, while exactly $q^n-1$ choices of $f_1$ and $q^{nm}-p$ choices of $g_1$ for the other cases of $(p,e)$.*

**Proof.** Let $0\neq\alpha,\beta\in F_{q^{nm}}$ such that $f(\alpha)=g(\alpha,\beta)=0$. Then (15) with $a=0$ and $b\neq 0$ is that $f_1(\alpha)\neq \Lambda f_0(\alpha)$, and there are exactly $q^n-1$ choices of such $f_1(x)$ since the set of $f_1(x)\in F_q[x]$ with $\deg f_1 < n$ is one-to-one corresponding to $F_q[\alpha]=F_{q^n}$. For such an $f_1(x)$, (15) with $a=1$ is that

$$g_1(\alpha,\beta)\neq \Lambda g_0(\alpha,\beta)+\frac{g_0^{(x)}(\alpha,\beta)}{f_0^{(x)}(\alpha)}\gamma+\frac{b\beta g_0^{(y)}(\alpha,\beta)}{\alpha f_0^{(x)}(\alpha)}\gamma,$$

where $\gamma=f_1(\alpha)-\Lambda f_0(\alpha)\neq 0$, and there are exactly $q^{nm}-p$ choices of such $g_1(x,y)$ since $\beta g_0^{(y)}(\alpha,\beta)\neq 0$ and the set of $g_1(x,y)\in F_q[x,y]$ with $\deg_x g_1 < n$ and $\deg_y g_1 < m$ is one-to-one corresponding to $F_q[\alpha,\beta]=F_{q^{nm}}$. When $2=p<e$, (16) is that

$$f_1(\alpha)\neq \Lambda f_0(\alpha)+\alpha f_0^{(x)}(\alpha). \tag{19}$$

Since $\alpha f_0^{(x)}(\alpha)\neq 0$, there are $q^n-2$ choices of eligible $f_1$. Set

$$\delta=\Lambda g_0(\alpha,\beta)+\frac{g_0^{(x)}(\alpha,\beta)}{f_0^{(x)}(\alpha)}\gamma,\quad \eta=\frac{\beta g_0^{(y)}(\alpha,\beta)}{\alpha f_0^{(x)}(\alpha)}\gamma,\quad \text{and}\quad \xi=\beta g_0^{(y)}(\alpha,\beta).$$

Then (15) with $(a,b)=(1,0)$, (15) with $(a,b)=(1,1)$, (17) and (18) are respectively that

$$g_1(\alpha,\beta)\neq \delta,\delta+\eta,\delta+\xi,\delta+\eta+\xi.$$

Since $\eta\neq\xi$ by (19), $\eta\neq 0$ and $\xi\neq 0$, there are exactly $q^{nm}-4$ choices of such $g_1(x,y)$.

**Remark 2.** Theorem 3 shows that whether or not $\langle f(x), g(x,y)\rangle$ is a maximal periodic ideal of $R[x,y]$ only depends on the lowest two $p$-adic components of $f(x)$ and $g(x,y)$, i.e., $f_0(x)$, $f_1(x)$, $g_0(x,y)$ and $g_1(x,y)$, but does not depend on the other $p$-adic components. To construct a maximal periodic ideal of $R[x,y]$, we need select four polynomials over $F_q$, say $f_0$, $f_1$, $g_0$ and $g_1$, such that $f_0(x)$ and $g_0(x,y)$ generate a maximal periodic ideal of $F_q[x,y]$, and that $f_1(x)$ and $g_1(x,y)$ are independent on $f_0$ and $g_0$. By Lemma 4, there is a possibility close to 1 that (15)–(18) hold when we are given $f_0$ and $g_0$ and choose $f_1$ and $g_1$ at random, and the choice of $f_1$ and $g_1$ is nearly arbitrarily in their range, in particular for large $q$ and for large $nm$. In this sense, the choice of $f_0$ and $g_0$ is an essential step. Regard $f_0$, $g_0$, $f_1$ and $g_1$ as polynomials with coefficients in $\Sigma_R$, and select arbitrarily $f_i(x)$ and

$g_i(x,y)$ with $\deg f_i < \deg f_0$, $\deg_x g_i < \deg f_0$ and $\deg_y g_i(x,y) < \deg_y g_0$, $2 \leqslant i < e$, combining the $f_i(x)$ and $g_i(x,y)$ according to (3) and (4), then we get two generator polynomials of a maximal periodic ideal.

**Example 1.** Let $R=Z/(2^e)=GR(2^e,1)$, $e \geqslant 3$, $\Sigma_R=\{0,1\}$. Take $f_0(x)=x^2+x+1 \in F_2[x]$ and $g_0(x,y)=y^2+xy+1 \in F_2[x,y]$, then $\Phi f_0(x)=x^3+x^2+x$ and $\Phi g_0(x,y)=xy^3+y^2+xy$. Computing by (13) and (14), we have $\Lambda f_0(x)=0$ and $\Lambda g_0(x,y)=xy+y$. Now (15) with $(a,b)=(0,1),(1,0)$ and $(1,1)$ become

$$f_1 \neq 0, \quad yf_1+g_1 \neq y+xy, \quad \text{and} \quad g_1 \neq y+xy$$

and (16)–(18) become

$$f_1 \neq x, \quad yf_1+g_1 \neq y, \quad \text{and} \quad g_1 \neq y.$$

Since $\deg f_1 < 2$, we can take $f_1(x)=x+1$ and $g_1 \neq 0, y+xy, xy$ or $y$, or take $f_1(x)=1$ and $g_1 \neq xy, y+xy, 0$ or $y$. Take $f_1(x)=x+1$ and $g_1(x,y)=1$, and take arbitrarily $a_0, a_1, b_{00}, b_{01}, b_{10}$, and $b_{11}$ in $R$. Then by Theorem 3,

$$I=\langle x^2+(3+4a_1)x+3+4a_0, y^2+(1+4b_{11})xy+4b_{10}x+4b_{01}y+3+4b_{00}\rangle$$

is the characteristic ideal of a maximal periodic array with period $15 \times 2^{2(e-1)}$.

## Acknowledgements

The authors would like to thank the anonymous referees for their useful suggestion on Theorem 3 and Remark 2.

## References

[1] S. Boztas, R. Hammons, P.V. Kummar, 4-phase sequences with near optimal correlation properties, IEEE Trans. Inform. Theory 38 (3) (1992) 1101–1113.
[2] A.R. Calderbank, J.A. Sloane, Modular and p-adic cyclic codes, Design Codes Cryptography 6 (1995) 21–35.
[3] Z. Dai, Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials, J. Cryptology 5 (1992) 193–207.
[4] L. Hu, D.Y. Pei, Maximal periodic two-dimensional arrays over Galois rings, preprint, 2000, submitted for publication.
[5] J.C. Interlando, R. Palazzo, M. Elia, On the decoding of Reed–Solomon and BCH codes over integer residues rings, IEEE Trans. Inform. Theory 43 (3) (1997) 1013–1021.
[6] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, London, 1983.
[7] M. Liu, L. Hu, Properties of Groebner base and applications to doubly periodic arrays, J. Symbolic Comput. 26 (1998) 301–314.
[8] P.Z. Lu, On Macaulay's inverse systems over QF rings, Chinese Ann. Math. 22A (2) (2000) 217–222.
[9] B.R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.
[10] G. Norton, On $n$-dimensional sequences I, J. Symbolic Comput. 20 (1995) 71–92.
[11] S. Sakata, A general theory of two-dimensional linear recurring arrays over an arbitrary finite field, IEEE Trans. Inform. Theory 24 (5) (1978) 719–730.

[12] P. Udaya, M.U. Siddiqi, Optimal biphase sequences with large linear complexities derived from ML-sequences over Z_4, IEEE Trans. Inform. Theory 42 (1) (1996) 206–216.
[13] P.V. Kumar, T. Helleseth, A.R. Calderbank, A.R. Hammons Jr., Large families of quaternary sequences with low correlation, IEEE Trans. Inform. Theory 42 (3) (1996) 579–592.
[14] Y.F. Zhu, A criteria of primitive polynomials over Galois rings, Acta Math. Sinica 39 (6) (1996) 783–788 (in Chinese).